Partner Eligibility

1. The partner should have performed at least 1 cloud security assessments in the past 3 years, preferably for BFSI customers. (Evidence/References to be submitted)
2. The partner should be able to propose a team which has hands-on experience in both AWS/Azure/GCP. (Resume of the team members to be submitted)
3. The partner should agree that the bank would interview the team members and would request for a replacement of any team member before or during the project execution

Scope of Work

Environment Scope:

Below is the cloud environment in scope: -

1. AWS (10-15 Accounts)
2. Azure (1-5 Subscriptions)
3. GCP (1-5 Projects)
4. Office365

Below includes but does not limit the overall domains in scope: -

- Identity & Access Management
- Network and Infrastructure
- Threat & Vulnerability Management
- Business Continuity & Disaster Recovery
- Privacy & Data Protection
- Regulatory & Policy Compliance
- Visibility & Incident Response
- Logging and Monitoring
- Cloud native workloads

Below includes but does not limit the overall activities in scope: -

- Review the ISSP policy/standards and its implication to the Bank's cloud environment.
- Understand the existing cloud security controls implemented at the bank.
- Review and understand the bank's cloud security related processes.
- Evaluate each cloud accounts against an exhaustive security checklist which covers all required controls as well as well-known industry standards.
- Leverage bank approved scanning tools to collect the required information if required.
- Propose changes to the policies/process/technology to better secure the cloud environment.

The partner may propose additional areas if relevant in their proposal. Also, should refine the areas with the granular activities that would be taken up as well as highlight the assumptions/exclusions if any.